SECRET

DD/A Registry
~~83-0596/4~~

ROUTING AND RECORD SHEET

83-0596/4

SUBJECT: (Optional)
Hostile Intelligence Services Threat and Evaluation of U.S. Countermeasures -- A National Assessment

FROM:
Director of Security
4E-60, Hqs.

EXTENSION

NO.

25X1

DATE
25 AUG 1983

25X1

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. DDA 7D-18, Hqs.				DD/A REGISTRY FILE: 10-1
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				Regraded Unclassified when separated from Classified Attachment(s)
15.				

FORM 1-79 610 USE PREVIOUS EDITIONS

SECRET

25 AUG 1983

MEMORANDUM FOR: Chief, Community Counterintelligence Staff
Intelligence Community Staff

VIA: Deputy Director for Administration

FROM: [redacted] 25X1
Director of Security

SUBJECT: Hostile Intelligence Services Threat and Evaluation of U.S. Countermeasures -- A National Assessment [redacted] 25X1

1. Forwarded herewith is this Office's response to the call for a first draft of subject 1983 National Assessment. A separate Directorate of Administration input is being provided by the Agency's Office of Communications. [redacted] 25X1

2. Where possible, our input tracks the Terms of Reference which were forwarded with the tasking. In order to avoid duplication of effort, we have addressed for the most part only those items which have changed since 1982. In addition, and specifically with reference to Section IV.D. (2-9) and Section IV.E., we would note simply that those issues were covered in detail in the recently published (July 1983) Countermeasures Organizational Study. We find much of the information developed during that Study directly applicable to this current effort. [redacted] 25X1

3. We are prepared to assist your Staff in providing additional data as necessary. If you have any questions concerning the attached input, please contact [redacted] Policy and Plans Group, [redacted] 25X1 25X1 25X1 25X1 25X1 25X1

OS 3 ~~2097~~ 2120

HOSTILE INTELLIGENCE SERVICES MULTIDISCIPLINARY THREAT AND U.S. COUNTERMEASURES

A NATIONAL ASSESSMENT

1983

CENTRAL INTELLIGENCE AGENCY

[redacted] 25X1

III.A.2.b. Advanced Technology - Automatic Data Processing Systems

The Office of Security, CIA, has continued its efforts to counter threats to the compromise of information processed and produced by automatic data processing systems. Since the last report, the proliferation of the personal computer has increased the threat of system penetrations by providing more sophisticated computing power to a larger community. These devices, with their capability to process off-line as well as tie into the mainframe systems as operative terminals, pose a wide-ranging and complex threat. 25X1

In addition, the improved storage media, i.e. floppy disks and large-capacity Winchester or permanent disk storage devices, have presented a most serious threat to security controls -- the floppy disks because of their small size and portability and the Winchester disks because of their large capacity and the difficulty and expense of sanitizing them. 25X1

Foreign Equipment. The Japanese continue to push the state of the art in computer technology by producing equipment which is powerful and expensive. This is particularly true in the personal computer field where, currently, the competition is fierce. The Japanese are also in the early stages of developing a new super computer with capabilities beyond the imagination just a few years ago. Of course, U.S. manufacturers (primarily IBM) are striving to meet this threat to their market. Regardless of which side wins the race, the threat of compromise will be magnified significantly by this development. The basic threat caused by the U.S. Government's use of foreign equipment has not changed, but it has been and will continue to be magnified. 25X1

Vendor Lack of Concern. Most computer manufacturers continue to ignore the security and privacy issues involved in the ADP field in their efforts to outdistance the competition. Some manufacturers are making the Data Encryption Standard (DES) available, while others are developing "front-end" security software/hardware systems. These efforts are encouraging; however, more in-depth research for the incorporation of protective features is needed. 25X1

Distributed Systems. Distributed processing deserves serious concern because of the capability to disperse a great volume of data at the local level for both storage and manipulation. This feature dilutes the security controls that can be effectively applied to system protection. Non-distributed

systems are limited in the amount of data which can be stored and manipulated locally by the buffer storage facility of the terminal. On the other hand, many personal or microcomputers now have high density Winchester disks and/or floppy disks which provide extended processing capabilities and high volume storage. Control of information is leaving the mainframe and being distributed to the remote system elements where it is more vulnerable to attack by hostile intelligence services. [redacted] 25X1

III.A.2.b. Advanced Technology - Technical Penetration

The capability of the opposition services to mount a technical threat against U.S. facilities, both foreign and domestic, continues to present serious concerns to the Intelligence Community. In Bloc countries the local government exercises total environmental control. Because embassies use local employees, that control extends to the embassy building itself. Under these circumstances, the opposition service can utilize many types of technical attack. [redacted] 25X1

In foreign countries, other than the Bloc, the threat of technical penetration by hostile intelligence, host country, or third party, can be equally as high. During the past eighteen months, there has been a marked increase in the number of Bloc governments that have acquired real estate and constructed official missions in close proximity to U.S. Government facilities. This increase has been especially prevalent in African nations. [redacted] 25X1

The technical threat to domestic facilities is perceived as increasing. [redacted] 25X1

The vulnerability to technical penetration is perceived as greater now due to the rapid proliferation of automatic data processing systems, office automation, and Sensitive Compartmented Information Facilities (SCIFs) in contractor facilities. [redacted] 25X1

III.A. Changes or Trends

° During the past year, the Soviets and other Bloc nations have continued to be active in working against U.S. facilities and

[redacted] 25X1

[redacted] 25X1

- It is CIA's and the Intelligence Community's assessment that with the new capabilities, the changing political climates, and the change in leadership of the Soviet Union, more attempts will be made to exploit vulnerabilities through technical penetrations. [redacted] 25X1

IV.B.6. Technical Threats - Audio and Electronic Penetrations

The CIA's technical security countermeasures program has as its objective, the detection and nullification of technical intelligence-gathering devices employed against Agency facilities overseas or in the United States. To accomplish this objective forty-one technical security officers: [redacted] 25X1

- Conduct on-site inspections of Agency and contractor facilities worldwide. [redacted] 25X1
- Promote professional exchange and coordination within the Intelligence Community on technical penetrations, procurements of technical equipment and development of technology and techniques. [redacted] 25X1
- [redacted] 25X1
- [redacted] 25X1

IV.B.6. Technical Threats - Computer

The CIA's Office of Security has presented a computer security plan for the 1980's which encompasses an increase in personnel as well as upgrading the skills of the people assigned to the field. This plan also includes an increase in research and development funding. The thrust of the plan is to use the improving capabilities of computer equipment in a positive mode; i.e., to develop security features which take advantage of state-of-the-art developments to increase the security posture of ADP systems. [redacted] 25X1

Current Efforts. The Office of Security is currently moving to publish: a revised Headquarters Regulation [redacted] 25X1 "Electronic Information Processing System Security"; the Headquarters Handbook [redacted] "Automatic Information 25X1 Processing System Security," which supports the regulation; a Headquarters Notice, "Control of Portable Magnetic Media"; a Headquarters Notice, "Personal Computers For Headquarters Applications"; and a book dispatch, "Personal Computers For Overseas Applications." It is anticipated that these documents will make the CIA user population more aware of computer security problems and provide the guidance to counter the threat. [redacted] 25X1

IV.C.2. Advanced Technology - Weaknesses - Audio and Electronic Penetrations

- Manpower resources are not adequate to address the expanding requirements in overseas areas; e.g., the Moscow Embassy project and other similar construction efforts which require technical monitoring; increased SCIF facilities in domestic areas need attention; and the demands for research and development in technical and physical security areas. [redacted] 25X1

- [redacted] 25X1

- Resource constraints have led to a severe shortage of qualified technical officers throughout the government. [redacted] 25X1

- Word processors and computer systems are being rapidly deployed overseas. These systems have not been totally evaluated to assess their vulnerability to technical exploitation. [redacted] 25X1

- Long-term underfunding of the Interagency Training Center (ITC) has resulted in the deterioration of the physical plant and equipment. This, in turn, has placed the ITC in the position of not being adequately equipped or staffed to conduct training classes on newly developed technical equipment, i.e., word processors, computers and computer-controlled telephone systems. [redacted] 25X1

IV.C.2. Advanced Technology - Strengths - Computer Security

Research and Development. The Office of Security is funding or plans in the future to fund the following research efforts:

Programmed for FY 83

Provably secure operating system - funds provided by the Office of Security through the Department of Defense. [redacted] 25X1

Encryption techniques for data protection on magnetic media. [redacted] 25X1

Security-approved degausser for ADP removable disks. [redacted] 25X1

Programmed for FY 84

Security filtering in distributed computer networks. [redacted] 25X1

Analysis of audit trails. [redacted] 25X1

Degausser for fixed magnetic media. [redacted] 25X1

Programmed for FY 85

On-line data base encryption. [redacted] 25X1

Tamper-proof detection design for computer peripheral devices. [redacted] 25X1

Emergency destruction of magnetic media. [redacted] 25X1

Computer hardware verification. [redacted] 25X1

V.A. Adequacy of Countermeasures Coverage - Audio and Electronic Penetrations and Computers

The adequacy of countermeasures depends on the commitment of resources, both monetary and manpower. Improvements should be addressed in areas such as:

- Increased CIA manpower ceilings to permit employment of 50 technical security officers. [redacted] 25X1
- Improved specialist pay scales to facilitate retention of experienced personnel. [redacted] 25X1
- Increased billets and funding to permit additional regional teams of technical security officers overseas. [redacted] 25X1
- Additional funding for R&D of technical security equipment to meet the technical threat of computer systems, word processors and computer-controlled office equipment. Continued research in document controls and copy prevention should be encouraged. [redacted] 25X1
- [redacted] 25X1
- Long-term commitment of resources to the ITC to provide it with state-of-the-art technology. [redacted] 25X1

Date

ROUTING AND TRANSMITTAL SLIP

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. A/EO/DDA	DJF	26 AUG 1983
2.		29 AUG 1983
3. DDA		29 AUG 1983
4.		
5.		

	Action		File		Note and Return
	Approval		For Clearance		Per Conversation
	As Requested		For Correction		Prepare Reply
	Circulate		For Your Information		See Me
	Comment		Investigate		Signature
	Coordination		Justify		

REMARKS

This looks like a good paper

Ar

DO NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

FROM: (Name, org. symbol, Agency/Post)	Room No.—Bldg.
	Phone No.

5041-102

OPTIONAL FORM 41 (Rev. 7-76)
Prescribed by GSA
FPMR (41 CFR) 101-11.206

☆ GPO : 1981 O - 361-529 (148)